

Identifikátor materiálu: **ICT-2-03**

Předmět – Téma sady	Informační a komunikační technologie
Téma materiálu	Antivirová ochrana, viry
Autor	Ing. Bohuslav Nepovím
Anotace	Student si procvičí / osvojí počítačové infiltrace.
Druh učebního materiálu	Prezentace (Výklad / Test)
Typ vzdělávání	Střední škola / SOU
Ročník	1. – 3.
Datum vytvoření	Říjen 2012

Informační a komunikační technologie

Antivirová ochrana, viry

Počítačový virus

Počítačová infiltrace - jakýkoliv neoprávněný vstup do počítačového systému a tím i do jeho dat (soubory, programy...).

Počítačový virus je taková forma počítačové infiltrace, která má schopnost vlastního množení a infikování dalších systémů bez vědomí uživatele.

Škála destruktivní činnosti, nejobvyklejšími ničivými akcemi virů je vymazání souborů, přeformátování disku, modifikace dat, přepis tabulky rozdělení disku (FAT), zničení této tabulky, označování sektorů za vadné, přepsání boot sektoru nebo zpomalení práce systému, nestabilita systému, krádež dat, šifrování dat, atd.

Dělení virů podle umístění v paměti

- ***Paměťově rezidentní viry***

Paměťově rezidentní virus setrvává ilegálně v paměti. Takový virus se většinou při prvním spuštění infikovaného souboru (pokud se jedná o souborový virus) nebo při prvním zavedení systému z infikovaného boot sektoru (pokud se jedná o boot virus) stane rezidentním v paměti, a odtud potom provádí svoji škodlivou činnost.

- ***Nerezidentní viry - viry přímé akce***

Tyto viry nevyužívají paměť pro své šíření. Stačí jim, když jsou aktivovány společně s hostitelským programem. Pak přebírají řízení jako první, provedou svoji činnost, nejčastěji replikaci a pak předají řízení zpět hostitelskému programu.

Dělení virů podle oblastí, které jsou napadeny

- **Boot viry** - tato první nejstarší skupina virů infikuje části nacházející se v určitých systémových oblastech disku. Těmito oblastmi mohou být: boot sektory disket a MBR (Master Boot Record) pevného disku. Napadením nějaké z těchto oblastí si boot virus zajistí svoje spuštění hned po startu počítače.
- **Souborové viry** - jak již z názvu vyplývá, jejich hlavním hostitelem jsou soubory.
- **Multipartitní viry** - jako viry multipartitní jsou označovány ty, které se chovají jako bootové viry, a zároveň jako viry souborové. Díky tomu jsou tyto viry "všestranné". Do této skupiny patří i populární virus OneHalf.
- **Makro viry**
tyto viry jsou tvořeny makry. Makra jsou programy, které si uživatel může vytvořit sám pro usnadnění práce v některých aplikacích (MS Office).

Techniky virů

- **Retro viry - odvetné viry** - Snaží se obejít a ještě lépe znemožnit práci antivirovým programům. Proto je mažou, vypínají rezidentní ochrany apod.
- **Neviditelné viry** - Stealth virus je rezidentní virus, který se pokouší vyhnout detekci skrytím projevů své přítomnosti v infikovaných souborech.
- **Kódované viry** - Prvotním účelem kódování bylo znepřehlednit vlastní kód viru a ztížit tak jeho analýzu.
- **Polymorfní (mutační) viry** - Polymorfní virus vytváří během replikace kopie, které jsou funkčně ekvivalentní, ale jednotlivé replikace se od sebe téměř úplně liší.
- **Metamorfní viry** - V napadeném souboru se totiž nenachází virus v klasickém smyslu. Napadený soubor totiž obsahuje jen kompilátor, společně se zdrojovým pseudokódem viru. Při spuštění infikovaného souboru vytvoří kompilátor v paměti novou, pokaždé odlišnou kopii viru.

Antivirové programy – detekce virů

Na počátku technologie skenování programů (zkráceně skenerů) byl nápad: *Vybrat z těla virů nějaké charakteristické skupiny instrukcí a takto získané sekvence použít pro hledání napadených programů.*

Antivirový program vyhledává a kontroluje data na základě virové databáze. V dnešní době vznikají nové viry a jejich mutace, tak rychle, že výrobce musí na tuto situaci reagovat 24 hodin denně. Tato virová databáze je tedy průběžně aktualizována a je k dispozici uživatelům ke stažení, což se většinou děje automaticky stažením z internetu.

Kvalitní skenery obsahují tzv. anti-stealth techniky, které dokážou obcházet aktivní stealth viry.

Skenery mohou být navíc ve dvou provedeních:

- ***paměťově rezidentní skener*** (*on-access scanner*)
on-access skener hlídá systém z operační paměti. Kontroluje veškerou činnost uživatele se soubory (kopírování, spouštění souborů) a pokud zjistí, že manipuluje s infikovaným programem, okamžitě ho na tuto skutečnost upozorní.
- ***skener "na požádání"*** (*on-demand scanner*)
Manuální typ skeneru. Uživatel obvykle definuje oblasti (pevný disk, adresář, disketa) které chce on-demand skenerem prohlédnout.

Nejúčinnější způsoby prevence

- Rezidentně spuštěný antivirový program, a to v jeho aktuální verzi
- Kontrola vložených datových medií antivirovým programem
- Kontrola souborů stažených z internetu
- Neotevírat přílohy emailu neznámého původu (soubory s příponou EXE, COM, BAT, VBS, SCR)
- Nezapomínat diskety v disketové mechanice (BOOT viry)
- Záloha dat
- Nepřeceňovat antivirový program

Přehled dnešních antivirů

AhnLab

avast!
be free

AVG.

AVIRA

Baidu 百度

Bitdefender

BullGuard

EMSI SOFT

'e Scan

eset

FORTINET.

F-Secure.

KASPERSKY

金山网络

LAVASOFT

McAfee
An Intel Company

Microsoft

PANDA
SECURITY

360
WWW.360.CN

SOPHOS

腾讯电脑管家
GUANJIA.QQ.COM

TREND
MICRO
Securing Your Journey to the Cloud

VIPRE

Srovnání antivirových programů

DLOUHODOBÉ VÝSLEDKY V TESTECH SPOLEČNOSTI VIRUS BULLETIN

Statistický přehled znázorňuje, kolikrát byl antivirový program testován, kolikrát z toho byl neúspěšný, kolikrát úspěšně našel všechny aktuálně vyskytující se viry a procento celkové úspěšnosti testovaného programu:

Antivirový program	Počet testů	Neúspěšný	Úspěšný	Procento úspěšnosti	
ESET - popis	93	2	91	97,8 %	Ceny
Norton (Symantec) - popis	66	8	58	87,9 %	Ceny
Avira - popis	63	5	58	92,1 %	Ceny
Sophos - popis	90	18	72	80,0 %	Ceny
TrustPort - popis	34	6	28	82,4 %	Ceny
Microsoft (produkty pro firmy)	43	2	41	95,3 %	
Kaspersky - popis	121	24	97	80,2 %	Ceny
BitDefender - popis	60	10	50	83,3 %	Ceny
F-Secure - popis	79	19	60	75,9 %	Ceny
Norman - popis	91	28	63	69,2 %	Ceny
McAfee - popis	76	24	52	68,4 %	Ceny
Avast! - popis	87	27	60	69,0 %	Ceny
AVG - popis	83	25	58	69,9 %	Ceny

Otázky:

- Co je počítačová infiltrace?
- Jaké je rozdělení virů podle umístění v paměti?
- Jaké je rozdělení virů podle oblastí, které jsou napadeny?
- Jaké jsou techniky virů?
- K čemu slouží antivirový program a jak funguje?
- Jaké antivirové programy znáte?

- **Použité zdroje:**

<http://www.skodlivysoftware.cz/informace>, [13.10.2012]

<http://www.antivirovecentrum.cz/antiviry.aspx>, [13.10.2012]

<https://www.antivirovecentrum.cz/aktuality/srovnani-antiviru.aspx>

<http://www.antivirovecentrum.cz/antiviry/katalog.aspx>, [13.10.2012]

<http://www.viry.cz/>, [13.10.2012]